UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,532	07/14/2001	Antony John Rogers	063170.6291	3485

5073 7590 07/07/2008

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
07/07/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	09/905,532	ROGERS ET AL.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,8-16 and 20-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,8-16 and 20-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 4, 8-16, and 20-23 are pending.

2. Response filed 04/30/2008 has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 4, 10-16, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chess (US 6192512) in view of Chambers (US 5398196).

As per claims 1, 10, 11, 12, and 14, Chess discloses a method of detecting viral code in subject files, comprising: creating an artificial memory region spanning one or more components of the operating system (see Fig. 2 column 4 lines 49-51); emulating execution of at least a portion of computer executable code in a subject file (see column 4 lines 33-49); detecting an attempt by the emulated computer executable code to access the artificial memory region; and determining based on the attempt to access the artificial memory region that the emulated computer executable code is viral (see column 4 lines 49-54).

Chess fails to explicitly disclose monitoring operating system calls by the emulated computer executable code to detect an attempt to access the artificial memory region.

However, Chambers teaches such monitoring (see column 6 line 60 through column 7 line 15).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to monitor the operating system calls of the Chess system.

Motivation to do so would have been to detect viral activity and report the status of all operating system requests performed by the program (see Chambers column 7 lines 55-60).

As per claims 4 and 16, the modified Chess and Chambers system discloses emulating functionality of the identified operating system call while monitoring the operating system call to determine whether the computer executable code is viral (see Chess column 4 lines 33-54).

As per claims 13 and 15, the modified Chess and Chambers system discloses a fourth segment comprising auxiliary code, wherein the auxiliary code determines an operating system call that the emulated computer executable code attempted to access; a fifth segment comprising analyzer code, wherein the analyzer code monitors the operating system call to determine whether the computer executable code is viral, while emulation continues (see Chess column 4 lines 33-54).

As per claim 21, the modified Chess and Chambers system discloses monitoring accesses by the emulated computer executable code to the artificial memory region to

detect looping; and determining based on the detection of looping that the emulated computer executable code is viral (see Chambers column 10 lines 40-58).

As per claim 22, the modified Chess and Chambers system discloses creating an artificial memory region comprises creating a custom version of an export table with predetermined values for the entry points (see Chambers column 9 lines 14-54).

5. Claims 8, 9, 20 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Chess and Chambers system as applied to claims 1 and 14 above, in view of Swift (US 6308274).

As per claims 8, 9, 20 and 23, the modified Chess and Chambers system fails to disclose monitoring access by the emulated computer executable code to dynamically linked functions to determine viral activity.

However, Swift teaches preventing access to dynamically linked functions to prevent the spread of viruses (see column 13 lines 16-43).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to monitor accesses (either direct or through jump tables) to dynamically linked functions in the emulation system of Chess and Chambers.

Motivation to do so, as recognized by one of ordinary skill in the art, would have been that DLLs are a common way viruses spread.

Response to Arguments

6. Applicant's arguments filed 04/30/2008 have been fully considered but they are not persuasive. Applicant argues Chambers does not disclose monitoring operating

system calls by the emulated computer executable code Golan fails to disclose monitoring accesses to DLLs.

With respect to Applicant's argument that Chambers does not disclose monitoring operating system calls by the emulated computer executable code, the monitor of Chambers is executed whenever an operating system is called to execute a program. This program monitors the target program (i.e. emulated computer executable code) to see if it is attempting to access memory selected for controlled access. This memory includes operating system procedures and data areas with certain addresses. When an instruction attempts to access the memory this is logged (see column 7 lines 16-32 and column 8 lines 3-35). As shown by the provided definition of "system call" from FOLDOC, when an application program (i.e. the program being emulated in Chambers) wants to access hardware (e.g. memory) it issues a system call to request the service from the operating system. Therefore, since the operating system provides access to memory via system calls and these accesses are monitored, Chambers teaches monitoring operating system calls by the emulated computer executable code.

With respect to Applicant's argument that Golan fails to teach monitoring accesses to DLLs, Golan was not relied upon to teach this limitation, Swift was previously provided to teach this limitation.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137